



1
2
3
4

Document Identifier: DSP0232

Date: 2014-12-22

Version: 1.2.0

5 **DASH Implementation Requirements**

6 **Supersedes: 1.1.0**

7 **Document Type: Specification**

8 **Document Class: Normative**

9 **Document Status: Published**

10 **Document Language: en-US**

11

12 Copyright Notice

13 Copyright © 2009, 2014 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

14 DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems
15 management and interoperability. Members and non-members may reproduce DMTF specifications and
16 documents, provided that correct attribution is given. As DMTF specifications may be revised from time to
17 time, the particular version and release date should always be noted.

18 Implementation of certain elements of this standard or proposed standard may be subject to third party
19 patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations
20 to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose,
21 or identify any or all such third party patent right, owners or claimants, nor for any incomplete or
22 inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to
23 any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize,
24 disclose, or identify any such third party patent rights, or for such party's reliance on the standard or
25 incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any
26 party implementing such standard, whether such implementation is foreseeable or not, nor to any patent
27 owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is
28 withdrawn or modified after publication, and shall be indemnified and held harmless by any party
29 implementing the standard from any and all claims of infringement by a patent owner for such
30 implementations.

31 For information about patents held by third-parties which have notified the DMTF that, in their opinion,
32 such patent may relate to or impact implementations of DMTF standards, visit
33 <http://www.dmtf.org/about/policies/disclosures.php>.

34

35

CONTENTS

36 Foreword 5

37 Introduction..... 6

38 1 Scope 7

39 2 Normative references 7

40 2.1 Approved references..... 7

41 2.2 Other references 9

42 3 Terms and definitions 10

43 4 Symbols and abbreviated terms..... 11

44 5 Mandatory profiles and specifications 12

45 6 Optional profiles 13

46 7 Protocol implementation requirements..... 14

47 7.1 Management protocol 14

48 7.2 Transport protocol..... 17

49 8 Security implementation requirements 17

50 8.1 Transport requirements..... 17

51 8.2 Roles and authorization 18

52 8.3 User account management..... 19

53 8.4 Authentication mechanisms 20

54 9 Discovery requirements..... 20

55 9.1 Network endpoint discovery stage..... 20

56 9.2 Management Access Point (MAP) discovery stage..... 20

57 9.3 Enumeration of management capabilities stage..... 22

58 9.4 RegisteredSpecification instance..... 22

59 10 In-band and out-of-band traffic requirements..... 23

60 ANNEX A (informative) Change log 24

61 Bibliography 25

62

63 Tables

64 Table 1 – Mandatory profiles and specifications..... 12

65 Table 2 – Optional profiles 13

66 Table 3 – WS-Transfer operations 14

67 Table 4 – WS-Enumeration operations..... 15

68 Table 5 – WS-Eventing operations 16

69 Table 6 – WS-Eventing message security recommendations 16

70 Table 7 – Required cryptographic algorithms or cipher suites..... 18

71 Table 8 – Operational roles supported by DASH..... 18

72 Table 9 – User account operations 19

73 Table 10 – Authentication mechanisms 20

74 Table 11 – WS-Management IdentifyResponse payload elements..... 21

75 Table 12 – CIM_RegisteredSpecification element requirements..... 23

76

78

Foreword

79 The *DASH Implementation Requirements* (DSP0232) was prepared by the Desktop and Mobile Working
80 Group of the DMTF.

81 DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems
82 management and interoperability.

83 Acknowledgments

84 The authors wish to acknowledge the following people.

85 Editors:

- 86 • Hemal Shah – Broadcom Corporation
- 87 • Joe Kozlowski – Dell Inc.
- 88 • Steven Breed – Dell Inc.

89 Contributors:

- 90 • Stephen Fong – Advanced Micro Devices
- 91 • Bob Blair – Advanced Micro Devices
- 92 • Paul Vancil – Advanced Micro Devices
- 93 • Simon Assouad – Broadcom Corporation
- 94 • Murali Rajagopal – Broadcom Corporation
- 95 • Jon Hass – Dell Inc.
- 96 • Rick Landau – Dell Inc.
- 97 • Christoph Graham – Hewlett-Packard Company
- 98 • Jeff Hilland – Hewlett-Packard Company
- 99 • David Hines – Intel Corporation
- 100 • Joel Clark – Intel Corporation
- 101 • Andy Currid – NVIDIA Corporation
- 102 • Steve Hand – Symantec Corporation
- 103 • Jim Davis – WBEM Solutions

104

105

Introduction

106 This specification describes the conformance requirements for implementing the Desktop and Mobile
107 Architecture for System Hardware (DASH) version 1.2.

108

DASH Implementation Requirements

109 1 Scope

110 This document describes the requirements for implementing the Desktop and Mobile Architecture for
111 System Hardware version 1.2. This document does not define the implementation requirements directly.
112 In clause 5, the mandatory profile specifications to be implemented are defined. In clause 6, the optional
113 and conditional profile specifications are defined. Clauses 7, 8, 9, and 10 define the protocol, security,
114 discovery, and management traffic requirements, respectively.

115 2 Normative references

116 The following referenced documents are indispensable for the application of this document. For dated
117 references, only the edition cited applies. For undated references, the latest edition of the referenced
118 document (including any amendments) applies.

119 2.1 Approved references

- 120 DMTF DSP0136, *Alert Standard Format Specification 2.0*,
121 http://www.dmtf.org/standards/documents/ASF/DSP0136_2.0.pdf
- 122 DMTF DSP0200, *CIM Operations over HTTP 1.3*,
123 http://www.dmtf.org/standards/published_documents/DSP0200_1.3.pdf
- 124 DMTF DSP0226, *Web Services for Management 1.0*,
125 http://www.dmtf.org/standards/published_documents/DSP0226_1.0.pdf
- 126 DMTF DSP0227, *WS-Management CIM Binding Specification 1.0*,
127 http://www.dmtf.org/standards/published_documents/DSP0227_1.0.pdf
- 128 DMTF DSP0230, *WS-CIM Mapping Specification 1.0*,
129 http://www.dmtf.org/standards/published_documents/DSP0230_1.0.pdf
- 130 DMTF DSP1009, *Sensors Profile 1.0*,
131 http://www.dmtf.org/standards/published_documents/DSP1009_1.0.pdf
- 132 DMTF DSP1009, *Sensors Profile, 1.1*,
133 http://www.dmtf.org/standards/published_documents/DSP1009_1.1.pdf
- 134 DMTF DSP1010, *Record Log Profile, 2.0*,
135 http://www.dmtf.org/standards/published_documents/DSP1010_2.0.pdf
- 136 DMTF DSP1011, *Physical Asset Profile 1.0*,
137 http://www.dmtf.org/standards/published_documents/DSP1011_1.0.pdf
- 138 DMTF DSP1012, *Boot Control Profile 1.0*,
139 http://www.dmtf.org/standards/published_documents/DSP1012_1.0.pdf
- 140 DMTF DSP1013, *Fan Profile 1.0*,
141 http://www.dmtf.org/standards/published_documents/DSP1013_1.0.pdf
- 142 DMTF DSP1014, *Ethernet Port Profile, 1.0*,
143 http://www.dmtf.org/standards/published_documents/DSP1014_1.0.pdf

- 144 DMTF DSP1015, *Power Supply Profile 1.0*,
145 http://www.dmtf.org/standards/published_documents/DSP1015_1.0.pdf
- 146 DMTF DSP1015, *Power Supply Profile, 1.1*,
147 http://www.dmtf.org/standards/published_documents/DSP1015_1.1.pdf
- 148 DMTF DSP1016, *Telnet Service Profile, 1.0*,
149 http://www.dmtf.org/standards/published_documents/DSP1016_1.0.pdf
- 150 DMTF DSP1017, *SSH Service Profile, 1.0*,
151 http://www.dmtf.org/standards/published_documents/DSP1017_1.0.pdf
- 152 DMTF DSP1018, *Service Processor Profile, 1.1*,
153 http://www.dmtf.org/standards/published_documents/DSP1018_1.1.pdf
- 154 DMTF DSP1022, *CPU Profile 1.0*,
155 http://www.dmtf.org/standards/published_documents/DSP1022_1.0.pdf
- 156 DMTF DSP1023, *Software Inventory Profile 1.0*,
157 http://www.dmtf.org/standards/published_documents/DSP1023_1.0.pdf
- 158 DMTF DSP1024, *Text Console Redirection Profile 1.0*,
159 http://www.dmtf.org/standards/published_documents/DSP1024_1.0.pdf
- 160 DMTF DSP1025, *Software Update Profile 1.0*,
161 http://www.dmtf.org/standards/published_documents/DSP1025_1.0.pdf
- 162 DMTF DSP1026, *System Memory Profile 1.0*,
163 http://www.dmtf.org/standards/published_documents/DSP1026_1.0.pdf
- 164 DMTF DSP1027, *Power State Management Profile 1.0*,
165 http://www.dmtf.org/standards/published_documents/DSP1027_1.0.pdf
- 166 DMTF DSP1029, *OS Status Profile 1.0*,
167 http://www.dmtf.org/standards/published_documents/DSP1029_1.0.pdf
- 168 DMTF DSP1029, *OS Status Profile, 1.1*,
169 http://www.dmtf.org/standards/published_documents/DSP1029_1.1.pdf
- 170 DMTF DSP1030, *Battery Profile 1.0*,
171 http://www.dmtf.org/standards/published_documents/DSP1030_1.0.pdf
- 172 DMTF DSP1033, *Profile Registration Profile 1.0*,
173 http://www.dmtf.org/standards/published_documents/DSP1033_1.0.pdf
- 174 DMTF DSP1034, *Simple Identity Management Profile 1.0*,
175 http://www.dmtf.org/standards/published_documents/DSP1034_1.0.pdf
- 176 DMTF DSP1035, *Host LAN Network Port Profile 1.0*,
177 http://www.dmtf.org/standards/published_documents/DSP1035_1.0.pdf
- 178 DMTF DSP1036, *IP Interface Profile 1.0*,
179 http://www.dmtf.org/standards/published_documents/DSP1036_1.0.pdf
- 180 DMTF DSP1037, *DHCP Client Profile 1.0*,
181 http://www.dmtf.org/standards/published_documents/DSP1037_1.0.pdf
- 182 DMTF DSP1038, *DNS Client Profile 1.0*,
183 http://www.dmtf.org/standards/published_documents/DSP1038_1.0.pdf
- 184 DMTF DSP1039, *Role Based Authorization Profile 1.0*,
185 http://www.dmtf.org/standards/published_documents/DSP1039_1.0.pdf

- 186 DMTF DSP1040, *Watchdog Profile, 1.0*,
187 http://www.dmtf.org/standards/published_documents/DSP1040_1.0.pdf
- 188 DMTF DSP1054, *Indications Profile 1.0*,
189 http://www.dmtf.org/standards/published_documents/DSP1054_1.0.pdf
- 190 DMTF DSP1058, *Base Desktop and Mobile Profile 1.0*,
191 http://www.dmtf.org/standards/published_documents/DSP1058_1.0.pdf
- 192 DMTF DSP1061, *BIOS Management Profile 1.0*,
193 http://www.dmtf.org/standards/published_documents/DSP1061_1.0.pdf
- 194 DMTF DSP1070, *Opaque Management Data Profile 1.0*,
195 http://www.dmtf.org/standards/published_documents/DSP1070_1.0.pdf
- 196 DMTF DSP1074, *Indicator LED Profile, 1.0*,
197 http://www.dmtf.org/standards/published_documents/DSP1074_1.0.pdf
- 198 DMTF DSP1075, *PCI Device Profile, 1.0*,
199 http://www.dmtf.org/standards/published_documents/DSP1075_1.0.pdf
- 200 DMTF DSP1076, *KVM Redirection 1.0*,
201 http://www.dmtf.org/standards/published_documents/DSP1076_1.0.pdf
- 202 DMTF DSP1077, *USB Redirection Profile 1.0*,
203 http://www.dmtf.org/standards/published_documents/DSP1077_1.0.pdf
- 204 DMTF DSP1086, *Media Redirection Profile 1.0*,
205 http://www.dmtf.org/standards/published_documents/DSP1086_1.0.pdf
- 206 DMTF DSP1108, *Physical Computer System View Profile, 1.0*,
207 http://www.dmtf.org/standards/published_documents/DSP1108_1.0.pdf
- 208 DMTF DSP1116, *IP Configuration Profile, 1.0*,
209 http://www.dmtf.org/standards/published_documents/DSP1116_1.0.pdf
- 210 DMTF DSP8007 *Platform Message Registry 1.0*,
211 http://schemas.dmtf.org/wbem/messageregistry/1/dsp8007_1.0.xml
- 212 DMTF DSP8030, DASH Namespace Schema 1.0, <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>
- 213 IETF RFC 2246, T. Dierks et al., *The TLS Protocol Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- 214 IETF RFC 4106, J. Viega and D. McGrew, *The Use of Galois/Counter Mode (GCM) in IPsec*
215 *Encapsulating Security Payload (ESP)*, <http://www.rfc-editor.org/rfc/rfc4106.txt>
- 216 IETF RFC 4301, S. Kent, *Security Architecture for the Internet Protocol*,
217 <http://www.rfc-editor.org/rfc/rfc4301.txt>
- 218 IETF RFC 4303, S. Kent, *IP Encapsulating Security Payload*, <http://www.ietf.org/rfc/rfc4303.txt>
- 219 IETF RFC 4346, T. Dierks et al., *The TLS Protocol Version 1.1*, <http://www.ietf.org/rfc/rfc4346.txt>
- 220 IETF RFC 5246, T. Dierks et al., *The TLS Protocol Version 1.2*, <http://www.ietf.org/rfc/rfc5246.txt>
- 221 **2.2 Other references**
- 222 ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*,
223 <http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype>

224 **3 Terms and definitions**

225 For the purposes of this document, the following terms and definitions apply.

226 **3.1**

227 **can**

228 used for statements of possibility and capability, whether material, physical, or causal

229 **3.2**

230 **cannot**

231 used for statements of possibility and capability, whether material, physical, or causal

232 **3.3**

233 **conditional**

234 indicates requirements to be followed strictly in order to conform to the document when the specified
235 conditions are met

236 **3.4**

237 **mandatory**

238 indicates requirements to be followed strictly in order to conform to the document and from which no
239 deviation is permitted

240 **3.5**

241 **may**

242 indicates a course of action permissible within the limits of the document

243 **3.6**

244 **need not**

245 indicates a course of action permissible within the limits of the document

246 **3.7**

247 **optional**

248 indicates a course of action permissible within the limits of the document

249 **3.8**

250 **shall**

251 indicates requirements to be followed strictly in order to conform to the document and from which no
252 deviation is permitted

253 **3.9**

254 **shall not**

255 indicates requirements to be followed in order to conform to the document and from which no deviation is
256 permitted

257 **3.10**

258 **should**

259 indicates that among several possibilities, one is recommended as particularly suitable, without
260 mentioning or excluding others, or that a certain course of action is preferred but not necessarily required

261 **3.11**

262 **should not**

263 indicates that a certain possibility or course of action is deprecated but not prohibited

264 **4 Symbols and abbreviated terms**

265 The following symbols and abbreviations are used in this document.

266 **4.1**

267 **ASF**

268 Alert Standard Format

269 **4.2**

270 **IANA**

271 Internet Assigned Numbers Authority

272 **4.3**

273 **IP**

274 Internet Protocol

275 **4.4**

276 **MAC**

277 Media Access Control

278 **4.5**

279 **MAP**

280 Management Access Point

281 **4.6**

282 **RMCP**

283 Remote Management and Control Protocol

284 **4.7**

285 **TCP**

286 Transmission Control Protocol

287 **4.8**

288 **TLS**

289 Transport Layer Security

290 **4.9**

291 **UDP**

292 User Datagram Protocol

293 **4.10**

294 **URI**

295 Uniform Resource Identifier

296 **4.11**

297 **WS**

298 Web Services

299 **5 Mandatory profiles and specifications**

300 The mandatory profiles and specifications shown in Table 1 shall be implemented in accordance with this
301 specification.

302 **Table 1 – Mandatory profiles and specifications**

Name	Number	Version	Description
<i>Base Desktop and Mobile Profile</i>	DSP1058	1.0	
<i>Profile Registration Profile</i>	DSP1033	1.0	
<i>Role Based Authorization Profile</i>	DSP1039	1.0	
<i>Simple Identity Management Profile</i>	DSP1034	1.0	
<i>WS-Management Specification</i>	DSP0226	1.0	
<i>WS-Management CIM Binding Specification</i>	DSP0227	1.0	
<i>WS-CIM Mapping Specification</i>	DSP0230	1.0	

303 **6 Optional profiles**

304 The optional profiles shown in Table 2 may be implemented. When a profile in Table 2 is implemented,
 305 the requirements specified in this clauses shall be met.

306 **Table 2 – Optional profiles**

Name	Number	Version	Description
<i>Battery Profile</i>	DSP1030	1.0	
<i>BIOS Management Profile</i>	DSP1061	1.0	
<i>Boot Control Profile</i>	DSP1012	1.0	
<i>CPU Profile</i>	DSP1022	1.0	
<i>DHCP Client Profile</i>	DSP1037	1.0	
<i>DNS Client Profile</i>	DSP1038	1.0	
<i>Ethernet Port Profile</i>	DSP1014	1.0	
<i>Fan Profile</i>	DSP1013	1.0	
<i>Host LAN Network Port Profile</i>	DSP1035	1.0	
<i>Indications Profile</i>	DSP1054	1.0	An instance of one of the concrete subclasses of CIM_Indication shall be the payload of a WS-Eventing message. The contents for AlertIndication should be drawn from <i>Platform Message Registry</i> (DSP8007). It is recommended that any vendor-specific messages are formulated with a published message registry with the owning entity other than the DMTF. Vendor-specific messages should be defined in a vendor-specific message registry that is conformant with the DMTF Message Registry Schema, as defined in DSP4006 .
<i>Indicator LED Profile</i>	DSP1074	1.0	
<i>IP Interface Profile</i>	DSP1036	1.0	
<i>IP Configuration Profile</i>	DSP1116	1.0	
<i>KVM Redirection Profile</i>	DSP1076	1.0	
<i>Media Redirection Profile</i>	DSP1086	1.0	
<i>Opaque Management Data Profile</i>	DSP1070	1.0	
<i>OS Status Profile</i>	DSP1029	1.0	
<i>OS Status Profile</i>	DSP1029	1.1	
<i>PCI Device Profile</i>	DSP1075	1.0	
<i>Physical Asset Profile</i>	DSP1011	1.0	
<i>Physical Computer System View Profile</i>	DSP1108	1.0	
<i>Power State Management Profile</i>	DSP1027	1.0	
<i>Power State Management Profile</i>	DSP1027	2.0	
<i>Power Supply Profile</i>	DSP1015	1.0	
<i>Power Supply Profile</i>	DSP1015	1.1	
<i>Record Log Profile</i>	DSP1010	2.0	
<i>Sensors Profile</i>	DSP1009	1.0	

Name	Number	Version	Description
<i>Sensors Profile</i>	DSP1009	1.1	
<i>Service Processor Profile</i>	DSP1018	1.1	
<i>Software Inventory Profile</i>	DSP1023	1.0	
<i>Software Update Profile</i>	DSP1025	1.0	
<i>SSH Service Profile</i>	DSP1017	1.0	
<i>System Memory Profile</i>	DSP1026	1.0	
<i>Telnet Service Profile</i>	DSP1016	1.0	
<i>Text Console Redirection Profile</i>	DSP1024	1.0	
<i>USB Redirection Profile</i>	DSP1077	1.0	
<i>Watchdog Profile</i>	DSP1040	1.0	

307 7 Protocol implementation requirements

308 A DASH-compliant implementation shall use a CIM-based data model for representing managed
 309 resources and services. This clause describes the Management Protocol and Transport Protocol
 310 requirements for a DASH implementation.

311 7.1 Management protocol

312 It is mandatory for DASH implementations to use the protocol defined in *Web Services for Management*
 313 *Specification* ([DSP0226](#)) as the management protocol for supporting operations. The implementation of
 314 the Web Services Management protocol shall expose CIM schema.

315 7.1.1 XML namespaces

316 The following URI identifies an XML namespace that contains DASH-specific XML definitions

317 (1) <http://schemas.dmtf.org/wbem/dash/1/dash.xsd>

318 7.1.2 WS-Transfer

319 It is mandatory for DASH implementations to support WS-Transfer as described in clause 7 of [DSP0226](#).
 320 Table 3 defines support for WS-Transfer operations and their respective DASH requirements.

321 **Table 3 – WS-Transfer operations**

Operation	Requirement	Notes
Get	Mandatory	This operation retrieves resource representations.
Put	Conditional	This operation updates resources. If an implemented profile requires ModifyInstance support, the Put operation shall be supported to fulfill that requirement.
Create	Conditional	This operation creates resource instances. If an implemented profile requires CreateInstance support, the Create operation shall be supported.
Delete	Conditional	This operation deletes resources. If an implemented profile requires DeleteInstance support, the Delete operation shall be supported.

322 **7.1.3 WS-Enumeration**

323 It is mandatory for DASH implementations to support WS-Enumeration as described in clause 8 of
 324 [DSP0226](#). Table 4 defines support for WS-Enumeration operations and their respective DASH
 325 requirements.

326 **Table 4 – WS-Enumeration operations**

Operation	Requirement	Messages
Enumerate	Mandatory	This operation is used to initiate an enumeration and receive an enumeration context.
Pull	Mandatory	This operation is used to pull a sequence of elements of a resource.
Renew	Optional	See Rule R8.1-4 in DSP0226 . Implementation of this operation is not recommended.
GetStatus	Optional	See Rule R8.1-4 in DSP0226 . Implementation of this operation is not recommended.
Release	Mandatory	This operation is used to release an enumeration context.
EnumerationEnd	Optional	See Rule R8.1-4 in DSP0226 . Implementation of this operation is not recommended.

327 It is recommended that the wsman:OptimizeEnumeration option be implemented as a child element of the
 328 wsen:Enumerate element. Refer to clause 8.2.3 of [DSP0226](#) for details. The service shall accept the
 329 element, but it does not have to honor it as described in Rule R8.2.3-1 of [DSP0226](#).

330 **7.1.3.1 WS-Enumeration Filter Dialects**

331 It is optional for DASH implementations to support Selector Filter Dialect for filtered enumeration and
 332 subscription as described in ANNEX E of [DSP0226](#). This recommendation does not contravene Rule
 333 R8.2.1-5 of [DSP0226](#).

334 It is optional for DASH implementations to support *Association Queries* with the dialect filter URI as
 335 specified in [DSP0227](#).

336 It is optional for DASH implementations to support the CQL filter dialect for enumeration as described in
 337 clause 7.1 of [DSP0227](#). This clause does not contravene Rule R8.2.1-5 of [DSP0226](#).

338 **7.1.4 WS-Eventing**

339 Support for WS-Eventing is conditional. A service advertising conformance to the *Indications Profile* shall
 340 support WS-Eventing as described in clause 10 of [DSP0226](#) and is further constrained by the definition
 341 described in this clause 7.1.4. Table 5 defines support for WS-Eventing operations and their respective
 342 DASH requirements.

343 **Table 5 – WS-Eventing operations**

Operation	Requirement	Notes
Subscribe	Mandatory	
Renew	Mandatory	
Unsubscribe	Mandatory	
SubscriptionEnd	Optional	
GetStatus	Optional	See Rule R10.3-1 in DSP0226 . Implementation of this operation is not recommended.

344 **7.1.4.1 WS-Eventing messaging security**

345 For WS-Eventing the messaging security defined in Table 6 should be followed.

346 **Table 6 – WS-Eventing message security recommendations**

Plane	WS-Eventing Message	Recommended Security Class	Security Principal Requiring Authentication
Control	wse:Subscribe	Class B as defined in clause 8.1, because it can carry sensitive information	Subscriber
	wse:Renew	Class B, because it can carry sensitive information	Subscriber
	wse:SubscriptionEnd	Class B, because it can carry sensitive information	Subscriber
	wse:Unsubscribe	Class B, because it can carry sensitive information	Subscriber
Delivery	wse:Delivery (Push)	Class A or B as defined in clause 8.1 (B for sensitive information or for more compute-intensive information)	MAP, but not necessarily with its own credentials
	wse:Delivery (PushWithAck)	Class A or B (B for sensitive information)	MAP, but not necessarily with its own credentials
	wse:Delivery (Batched)	Class A or B (B for sensitive information)	MAP, but not necessarily with its own credentials
	wsen:Pull (Pull delivery)	Class A or B (B for sensitive information)	Subscriber

347 7.1.4.2 WS-Eventing delivery mode

348 DASH implementations shall support WS-Eventing Push Mode as described in clause 10.2.9.2 of
349 [DSP0226](#). DASH implementations should support WS-Eventing PushWithAck Mode as described in
350 clause 10.2.9.3 of [DSP0226](#).

351 7.1.4.3 Subscription related property definition guidance

352 The PersistenceType property in a CIM_ListenerDestination instance created internally in response to
353 wse:Subscribe should be set to 3 (Transient).

354 The value for the FailureTriggerTimeInterval property on the CIM_IndicationSubscription or
355 CIM_FilterCollectionSubscription instance created internally in response to wse:Subscribe should be to
356 30 seconds.

357 7.2 Transport protocol

358 DASH implementations shall use HTTP 1.1 as the SOAP transport for [DSP0226](#). For detailed information
359 about the transport protocol required by DASH, refer to clause 5.2 of the *Systems Management*
360 *Architecture for Mobile and Desktop Hardware White Paper* ([DSP2014](#)).

361 8 Security implementation requirements

362 This clause describes transport requirements, roles and authorization, user account management, and
363 authentication.

364 8.1 Transport requirements

365 DASH defines two security classes for HTTP 1.1 transport:

- 366 1) **Class A:** The security class A requires HTTP digest authentication for the user authentication.
367 For this class, no encryption capabilities are required beyond the encryption of the password
368 during the digest authentication exchange. If class A is implemented, MD5 digest algorithm shall
369 be supported.
- 370 • **String = "HTTP_DIGEST"**
 - 371 • URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest>
 - 372 2) **Class B:** This class defines three security profiles that are based on either TLS or IPsec with
373 specifically selected modes and cryptographic algorithms. For class B compliance, the support
374 for at least one of the following security profiles is mandatory:
 - 375 • **String = "HTTP_TLS_1"**
 - 376 • URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest>
 - 377 • **String = "HTTP_TLS_2"**
 - 378 • URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic>
 - 379 • **String = "HTTP_IPSEC"**
 - 380 • URI = <http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest/ipsec>

381 A DASH implementation shall support at least one of the preceding security classes. It is recommended
382 that a DASH implementation be Class B compliant for privacy/confidentiality and additional security.

383 Refer to 7.1.4.1 for WS-Eventing security requirements.

384 **8.1.1 Cryptographic algorithms and cipher suites**385 Table 7 lists the required cryptographic algorithms or cipher suites for the security profiles mentioned in
386 this section.387 **Table 7 – Required cryptographic algorithms or cipher suites**

Security Profile	Required Algorithm(s) or Cipher suite	Notes
"HTTP_DIGEST"	MD5	
"HTTP_TLS_1"	TLS_RSA_WITH_AES_128_CBC_SHA (for TLS) and MD5 (for HTTP digest)	TLS version 1.0 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268. It is recommended that the latest 1.x version of TLS is implemented.
"HTTP_TLS_2"	TLS_RSA_WITH_AES_128_CBC_SHA	TLS version 1.0 or later Refer to RFC 2246, RFC 4346, RFC 5246 and RFC 3268. It is recommended that the latest 1.x version of TLS is implemented.
"HTTP_IPSEC"	For IPsec: AES-GCM (key size: 128 bits, ICV or Digest len: 16 B) or AES-CBC (Key size: 128 bits) with HMAC-SHA1-96 and For HTTP digest: MD5	Refer to RFC 4301 , 4303 , and 4106

388 **8.2 Roles and authorization**389 Table 8 outlines the Operational Roles supported by DASH implementations and the respective DASH
390 requirements.391 **Table 8 – Operational roles supported by DASH**

Operational Role	Requirement	Notes
Read-only User	Optional	For detailed description of these roles see DSP2014 .
Operator	Optional	
Administrator	Mandatory	

392 A DASH-compliant service shall support the administrator role. An implementation may support the
393 operator and/or read-only user roles. All roles shall be modeled using [DSP1039](#), *Role Based*
394 *Authorization Profile, 1.0*.

395 **8.3 User account management**

396 The authentication and authorization mechanisms defined are tied with user account management. DASH
 397 implementations shall support a role-based authorization model.

398 Each user shall have the ability to modify its own account credentials, depending on the user’s privileges.
 399 An account in the administrator role shall be able to perform account management for all users. Table 9
 400 outlines the operations supported for user account management and the respective DASH requirements.

401 **Table 9 – User account operations**

Operation	Requirement	Notes
Create an account	Optional	Recommended for the administrator role
Delete an account	Optional	Recommended for the administrator role
Enable an account	Optional	
Disable an account	Optional	
Modify the privileges of an account	Optional	
Modify the password of an account	Mandatory	Required for the administrator account.
Change the role of an account	Optional	
Create a group of accounts	Optional	
Delete a group of accounts	Optional	
Add an account to a group	Optional	
Remove an account from a group	Optional	
Change the role of a group	Optional	
Modify the privileges of a group	Optional	
Change the associations of roles and accounts	Optional	Recommended for the administrator role

402 The modifications of privileges include the changing of bindings between accounts or groups and roles.
 403 All operations defined in Table 9 shall be performed using operations as defined in DMTF [DSP1039](#), *Role*
 404 *Based Authorization Profile, 1.0* and DMTF [DSP1034](#), *Simple Identity Management Profile, 1.0*.

405 8.4 Authentication mechanisms

406 DASH implementations shall support User-Level authentication. DASH implementations may support two-
407 level (Machine-Level and User-Level) authentication.

408 Table 10 outlines requirements for the three types of authentication mechanisms supported by DASH 1.0
409 implementations.

410 **Table 10 – Authentication mechanisms**

Authentication Mechanisms	Requirement	Notes
Machine-Level	Optional	
User-Level	Mandatory	
Third-Party	Optional	

411 9 Discovery requirements

412 Multiple discovery stages are required to accumulate the necessary information from the managed
413 system. This clause defines the implementation requirements of the stages involved in discovering
414 managed systems and their management capabilities.

415 9.1 Network endpoint discovery stage

416 Clause 8.2 of the *Systems Management Architecture for Mobile and Desktop Hardware White Paper*
417 ([DSP2014](#)) describes endpoint discovery methods. A DASH 1.1 compliant implementation need not
418 support any of the described methods.

419 9.2 Management Access Point (MAP) discovery stage

420 A DASH-compliant MAP should support the following phase process for MAP discovery:

- 421 • **Phase 1:** RMCP Presence Ping/Pong.

422 A DASH-compliant MAP shall support the following phase process for MAP discovery:

- 423 • **Phase 2:** WS-Management Identify method.

424 9.2.1 RMCP Presence Ping/Pong

425 Presence Ping is an RMCP command that is defined in the *Alert Standard Format Specification*,
426 ([DSP0136](#)). The command involves a request-response message exchange initiated by a management
427 client (Ping) and completed by a management service (Pong).

428 The format of the RMCP Presence Pong (40h) data section shall conform to clause 3.2.4.3 of [DSP0136](#)
429 with the following definition:
430

431 *Supported Interactions* field (Data Byte 10 of Presence Pong), bit 5 set to 1b if DASH is supported

432 A DASH-compliant MAP should support this command on the ASF-RMCP well-known UDP port (623)
433 and/or well-known UDP port (664).

434 **9.2.2 WS-Management Identify method**

435 Refer to clause 11 of [DSP0226](#) for a definition of the Identify method. A DASH-compliant management
 436 service shall support the Identify method on each TCP port on which WS-Management service is
 437 supported.

438 In addition to the child element defined in [DSP0226](#), the following extension elements are defined by
 439 DASH as children of the *IdentifyResponse* element:

```

440 <s:Body>
441   <wsmid:IdentifyResponse>
442     <wsmid:ProtocolVersion> xs:anyURI </wsmid:ProtocolVersion>
443     <wsmid:ProductVendor> xs:string </wsmid:ProductVendor>
444     <wsmid:ProductVersion> xs:string </wsmid:ProductVersion>
445     <dash:DASHVersion> xs:string </dash:DASHVersion>
446     <wsmid:SecurityProfiles>
447       <wsmid:SecurityProfileName> xs:string or URI </wsmid:SecurityProfileName> +
448     </wsmid:SecurityProfiles>
449   </wsmid:IdentifyResponse>
450 </s:Body>
    
```

451 Table 11 defines the IdentifyResponse payload requirements for DASH 1.1.

452 **Table 11 – WS-Management IdentifyResponse payload elements**

Element	Requirement	Notes
wsmid:IdentifyResponse	Mandatory	The body of the response
wsmid:IdentifyResponse/wsmid:ProtocolVersion	Mandatory	URI identifying DSP0226 1.0 http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
wsmid:IdentifyResponse/wsmid:ProductVendor	Optional	
wsmid:IdentifyResponse/wsmid:ProductVersion	Optional	
wsmid:IdentifyResponse/dash:DASHVersion	Mandatory	Identifies the version of the <i>DASH Implementation Requirements</i> specification that is supported, which shall be in the form “M.N.U”, where M represents major version, N represents minor version, and U represents update version of the specification. For this specification, the value shall be set to “1.1.0”.

Element	Requirement	Notes
wsmid:IdentifyResponse/wsmid:SecurityProfiles/ wsmid:SecurityProfileName	Mandatory	<p>URI identifying the security profile supported</p> <p>Class A:</p> <p>“HTTP_DIGEST”: http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest</p> <p>Class B:</p> <p>“HTTP_TLS_1”: http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest</p> <p>“HTTP_TLS_2”: http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic</p> <p>“HTTP_IPSEC”: http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest</p>

453 9.2.3 wsmid:Identify security implementation requirements

454 Implementations may support wsmid:Identify without authentication as described in Rule R11.4 of
 455 [DSP0226](#).

456 If an implementation supports wsmid:Identify without authentication, it should support it through a URL
 457 that contains the suffix "/wsman-anon/identify."

458 9.3 Enumeration of management capabilities stage

459 The DMTF *Profile Registration Profile* ([DSP1033](#)) specifies methods for enumerating the management
 460 capabilities of a CIM-based management access point in a scalable manner. Scalability here refers to the
 461 fact that each registered profile concisely describes support for a set of related management capabilities
 462 that is independent of the number of CIM instances supported by the management access point.

463 9.4 RegisteredSpecification instance

464 The DASH implementation should support an instance of CIM_RegisteredSpecification to indicate
 465 support for this version of the specification.

466 Table 12 identifies the element requirements for CIM_RegisteredSpecification.

467

Table 12 – CIM_RegisteredSpecification element requirements

Element	Requirement	Description
Properties		
InstanceID	Mandatory	Key, see schema definition.
SpecificationType	Mandatory	This property shall have a value of 3 ("Initiative Wrapper").
RegisteredOrganization	Mandatory	This property shall have a value of 2 (DMTF).
RegisteredName	Mandatory	This property shall have a value of "DASH".
RegisteredVersion	Mandatory	This property shall have a value of "1.2.0".
AdvertiseTypes	Mandatory	Required, see Schema definition.
AdvertiseTypeDescriptions	Mandatory	See Schema definition.
Operations		
GetInstance	Mandatory	
EnumerateInstances	Mandatory	
EnumerateInstanceNames	Mandatory	

468 The instance of CIM_RegisteredSpecification shall be exposed in the interop namespace. The instance to
 469 CIM_RegisteredSpecification shall be associated with at least one instance of CIM_RegisteredProfile of
 470 one of the mandatory profiles defined in this specification using an instance of
 471 CIM_ReferencedSpecification. The Antecedent property of the instance of CIM_ReferencedSpecification
 472 shall reference the instance of the CIM_RegisteredProfile. The Dependent property of the instance of
 473 CIM_ReferencedSpecification shall reference the instance CIM_RegisteredSpecification.

474 **10 In-band and out-of-band traffic requirements**

475 A DASH compliant service shall support, at minimum, a shared IPv4 and MAC address as defined below:

- 476 • A physical system’s out-of-band Management Access Point and the In-Band host shall share
 477 the MAC address and IPv4 address of the network interface. Manageability traffic shall be
 478 routed to the MAP through the well-known system ports defined by IANA. Implementations may
 479 support the use and configuration of other ports.

480 Developers may use any port necessary during product development. Implementations shall support the
 481 IANA-defined system ports for product deployment.

- 482 • Sideband: TCP ports for WS-Management Service
 - 483 – OOB-WS-HTTP
 - 484 • TCP 623
 - 485 – OOB-WS-HTTPS
 - 486 • TCP 664 (If class B is implemented)
- 487 • In-band: TCP ports for WS-Management Service may be supported on the following transport
 488 ports and shall be transport specific:
 - 489 – HTTP
 - 490 – HTTPS (If class B is implemented)

491 NOTE In-band and out-of-band MAPs shall listen on different ports.

492
493
494
495
496
497

ANNEX A
(informative)
Change log

Version	Date	Description
1.0.0	2009-05-19	
1.1.0	2009-06-22	DMTF Standard
1.2.0	2014-12-22	DMTF Standard

498

Bibliography

499

500 DMTF DSP2014, *Systems Management Architecture for Mobile and Desktop Hardware White Paper*
501 *1.1.0*, http://www.dmtf.org/standards/published_documents/DSP2014_1.1.0.pdf
502 (Informative text in this document details Protocol, Security, and Discovery.)

503 DMTF DSP4006, Standard Registry Development and Publication Process 1.1,
504 http://www.dmtf.org/standards/published_documents/DSP4006_1.1.0.pdf

505